

Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Name>>  
<<Address 1>>  
<<Address 2>>  
<<City>><<State>><<Zip>>

<<Date>>

Dear Current or Former Aurora Caregiver:

Aurora Health Care recently discovered that we were the target of a criminal cyber attack that infected some workstations and servers with malware, or a type of computer virus. The malware had been installed on some of Aurora's workstations and servers and was designed to capture login information when users accessed certain websites, mostly financial in nature and some social media. While we have no evidence to suggest that any caregiver sensitive information has been misused, I want to make sure you know what we are doing about it as an organization and what your role is in keeping information safe to help guard against similar incidents in the future.

As to the incident itself, on January 27, 2015, we discovered malware had been installed on certain Aurora workstations and servers. Immediately upon discovering this, we notified the FBI and launched an internal investigation, engaging one of the nation's premier cybersecurity firms to remove the malware and conduct a forensics analysis. In short, we wanted to understand what kind of information had potentially been accessed. The investigation concluded that the malware was designed to intercept active sessions and capture login information from the users of the affected workstations who had accessed certain websites. The websites that we know were targets are listed on Caregiver Connect and in the attached information.

While we believe that the malware has been removed and the system's security restored, we are alerting all caregivers of the incident and encouraging you to take certain precautionary measures.

As a first step, you should secure personal accounts by changing the passwords associated with websites, especially those containing sensitive information, which may have been accessed from Aurora computers.

**To further ensure the security of your information, we are also encouraging caregivers to take advantage of the complimentary one-year credit and identity monitoring services we are providing you through Experian's® ProtectMyID® Alert. A detailed description of this product with specific instructions on how to enroll for this service is included in the attached document entitled ProtectMyID® Membership.**

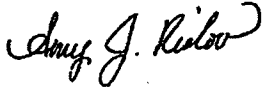
To help prevent an incident like this in the future, we have implemented additional safeguards, including the installation of upgraded audit and surveillance technologies to detect unauthorized intrusions and advanced encryption technologies to protect information assets, such as laptops that may contain sensitive information. Additionally, we are reinforcing our existing policies and processes and rolling out enhanced training and awareness programs for caregivers. Safeguarding information is a team activity. Just as we are implementing enhanced features, it is extremely important that you do everything you can to help prevent criminal cyber attacks. Change your work and personal passwords often and make sure they are strong. Never click on links or open attachments in email that look like spam. Don't access personal financial or social media websites from Aurora workstations, even if you are using it at home.

We apologize for any inconvenience or concern this incident may have caused you. Certainly, these types of criminal activities are harmful, costly and frustrating. We continue to work with the FBI to identify these hackers. We appreciate the trust each of you has in our organization, and we work hard every day to earn that trust.

And, while attacks such as this are, unfortunately, ever more common in our world today, each of us can make a difference in cybersecurity.

If you have any questions or concerns, please call 1-888-593-5904, Monday through Friday, between the hours of 8:00 a.m. and 8:00 p.m. Central, or email us at [InformationProtection@aurora.org](mailto:InformationProtection@aurora.org). We have also posted details regarding this matter and the ongoing investigation to Caregiver Connect.

Sincerely,

A handwritten signature in cursive script, reading "Amy J. Rislov". The signature is written in black ink and is positioned above the printed name and title.

Amy Rislov  
Chief Human Resources Officer

## ProtectMyID® Membership

To address this incident, we are offering you a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft.

### Activate ProtectMyID Now in Three Easy Steps

1. ENSURE that you enroll by June 10, 2015 (Your code will not work after this date.)
2. VISIT the ProtectMyID web site to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)
3. PROVIDE your activation code: [code]

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: PC92533.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)  
or call 877-288-8057 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## Additional Important Information

### Protecting Yourself

Please be aware that individuals may contact you via scam email or phone campaigns designed to capture personal information, known as "phishing." The scams may be designed to appear as if they are from Aurora. Aurora will not email your personal email account, nor will we call you at home unless we are responding to a request from you regarding this incident. Aurora is not calling caregivers regarding this incident and is not asking for credit card information or social security numbers over the phone.

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card, bank and other account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

### Other Available Resources

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information and to contact the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 9532  
Allen, TX 75013

TransUnion  
(800) 916-8800  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 6790  
Fullerton, CA 92834

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

**California Residents:** This notification has not been postponed at the request or as the result of a law enforcement investigation.

**Maryland Residents:** Maryland residents can obtain contact the Office of the Attorney General at:

Office of the Attorney General  
220 St. Paul Place, Baltimore, MD 21202  
(888) 743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**Massachusetts Residents:** Massachusetts residents have the right to obtain a police report, if any, filed in regard to this incident. Massachusetts law also allows Massachusetts consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above.

**North Carolina Residents:** North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office  
9001 Mail Service Center, Raleigh, NC 27699-9001  
(877) 566-7226  
[www.ncdoj.com](http://www.ncdoj.com)